ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 107 (2004) 266–281

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

On a certain family of generalized Laguerre polynomials

Elizabeth A. Sell

University of North Carolina at Chapel Hill, CB #3250, Phillips Hall, Chapel Hill, NC 27599, USA

Received 26 August 2003; revised 4 February 2004

Communicated by T.Y. Lam

Abstract

Following the work of Schur and Coleman, we prove the generalized Laguerre polynomial $L_n^{(-3-n)}(x) = \sum_{j=0}^{n} \frac{1}{j!} \frac{(n-j+1)(n-j+2)}{2} x^j$ is irreducible over the rationals for all $n \geqslant 1$ and has Galois group A_n if $n+1$ is an odd square, and S_n otherwise. We also show that for certain negative integer values of α and certain congruence classes of n modulo 8, the splitting field of $L_n^{(\alpha)}(x)$ can be embedded in a double cover.

Keywords: Generalized Laguerre polynomials; Newton polygons

1. Introduction

The nth degree generalized Laguerre polynomial in a variable x and a parameter α is defined as follows:

$$L_n^{(\alpha)}(x) = (-1)^n \sum_{j=0}^{n} \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!}.$$

These polynomials were first studied by Pólya and Szegő [14, p. 274]. Various mathematicians have studied their algebraic properties for certain rational values of α. Schur [15, No. 67, 70] proved the irreducibility of $L_n^{(\alpha)}(x)$ over $\mathbb{Q}$ and computed its Galois group for $\alpha = 0, \alpha = 1$, and $\alpha = -1-n$. Hajir [8] did the same for $\alpha = -2-n$, and Gow [7] computed the Galois group for $\alpha = n$, assuming $L_n^{(n)}(x)$ is

E-mail address: esell@email.unc.edu.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2004.03.004

irreducible. More broadly, Filaseta and Lam [6] proved that if α is a rational number which is not a negative integer, $L_n^{(\alpha)}(x)$ is irreducible for all but finitely many n. In [2], Coleman calculated the Newton polygon at an arbitrary prime p of the truncated exponential polynomial,

$$e_n(x) = L_n^{(-1-n)}(x) = \sum_{j=0}^{n} \frac{x^j}{j!}.$$

We begin by observing that Coleman's method gives a general criterion which establishes the irreducibility of a large number of $L_n^{(\alpha)}(x)$ (see Corollary 9). For the family $\alpha = -3 - n$, this method, when combined with an additional criterion of Filaseta [5] (also based on Newton Polygons), yields irreducibility for all n. We then apply Coleman's technique to compute the Galois group for $\alpha = -3 - n$.

In the remainder of this work, we study the problem of embedding the splitting field of $L_n^{(\alpha)}(x)$ for various rational α in a double cover. The solution of this problem is achieved by a theorem of Serre [17] which reduces the problem to the calculation of the Hasse–Witt invariant of a certain trace form associated to our polynomial, for which we have available certain complicated but explicit formulas due to Feit [4].

Notation. For any non-zero integer n, and prime p, $\mathrm{ord}_p(n)$ is the p-adic valuation of n, so that

$$n = \prod_p p^{\mathrm{ord}_p(n)}.$$

We set $\mathrm{ord}_p(0) = \infty$.

1.1. Newton polygons

Given a polynomial f with coefficients in $\mathbb{Q}_p$, we can attach to it, for each prime p, a geometric object known as the Newton polygon. This object will then specify the p-adic valuations of each root of f. As we will see below, this data can sometimes lead us to information about the factorization of f over $\mathbb{Q}$, assuming f has rational coefficients. The reader can find an introduction to this topic in [12] or [18].

Definition 1. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in $\mathbb{Q}_p[x]$, with $a_0a_n \neq 0$. The Newton polygon of f at p, denoted $\mathrm{NP}(f,p)$, is defined to be the lower convex hull in the Cartesian plane of the points

$$\{(0, \mathrm{ord}_p(a_0)), (1, \mathrm{ord}_p(a_1)), \ldots, (n, \mathrm{ord}_p(a_n))\}.$$

To construct the lower convex hull, follow this procedure: Plot all the points in the list above. Rotate the vertical line through $(x_0, y_0) := (0, \mathrm{ord}_p(a_0))$ counterclockwise until it reaches one of the other points; let (x_1, y_1) be the furthest point of type $(i, \mathrm{ord}_p(a_i))$ that lies on this line. Draw the straight line between (x_0, y_0) and (x_1, y_1).

Now rotate the vertical line through (x_1, y_1) counterclockwise until it reaches another point, and call the furthest point along this line (x_2, y_2). Continue this procedure until you reach $(a_n, \mathrm{ord}_p(a_n))$. It is clear that the slopes of the line segments should increase from left to right, and by construction, no two edges have the same slope. The union of the line segments is the lower convex hull.

The main theorem about the Newton Polygon is

Theorem 2. *Let* $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$ *denote the successive vertices of* $\mathrm{NP}(f, p)$. *Then there exist polynomials* $f_1, \ldots, f_r$ *in* $\mathbb{Q}_p[x]$ *such that*

(i) $f(x) = f_1(x)f_2(x)\cdots f_r(x)$,
(ii) *the degree of* f_i *is* $x_i - x_{i-1}$,
(iii) *all the roots of* f_i *in* $\overline{\mathbb{Q}_p}$ *have p-adic valuation* $-(\frac{y_i - y_{i-1}}{x_i - x_{i-1}})$.

Corollary 3 (Coleman). *Let d be a positive integer. Suppose d divides the denominator of each slope, in lowest terms, of* $\mathrm{NP}(f, p)$. *Then d divides the degree of each factor of f over* $\mathbb{Q}_p$.

Proof. Let h be an irreducible factor of f over $\mathbb{Q}_p$, and let α be a root of h. Recall that $\mathrm{ord}_p(\alpha)$ is in $\frac{1}{e}\mathbb{Z}$, where e is the index of ramification of the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$. Thus, since d divides the denominator of the p-adic valuation of α, d must divide e. But e divides $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$, which is precisely the degree of h. □

1.2. The Coleman criterion

Here we formulate a criterion restricting the degrees of factors of a polynomial in $\mathbb{Q}[x]$. This criterion was developed by Coleman [2] and then applied to prove the irreducibility of

$$e_n(x) = L_n^{(-1-n)}(x) = \sum_{j=0}^{n} \frac{x^j}{j!}.$$

Write n in base p, labelling only the non-zero digits:

$$n = b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_s p^{n_s}, \tag{1}$$

where $0 < b_i < p$, and $n_1 > n_2 > \cdots > n_s$. Now let $k_0 = 0$, and define

$$k_i = b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_i p^{n_i}, \quad 1 \leqslant i \leqslant s. \tag{2}$$

Proposition 4 (Coleman). *The vertices of* $\mathrm{NP}(e_n, p)$ *are* $(k_i, -\mathrm{ord}_p(k_i!))$, *for* $0 \leqslant i \leqslant s$. *Its slopes are*

$$m_i = \frac{-(p^{n_i} - 1)}{p^{n_i}(p-1)}, \quad 1 \leqslant i \leqslant s. \tag{3}$$

The proof is straightforward, using Legendre's formula: If $k = a_0 + a_1 p + \cdots + a_s p^s$ is the p-adic expansion of a positive integer k, then

$$\mathrm{ord}_p(k!) = \frac{k - (a_0 + a_1 + \cdots + a_s)}{p-1}.$$

A polynomial of the form $f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!}$ in $\mathbb{Q}[x]$ is called *Hurwitz-integral at p* if $\mathrm{ord}_p(a_j) \geqslant 0$ for $0 \leqslant j \leqslant n$. It is called *Hurwitz-integral* if $a_j \in \mathbb{Z}$ for $0 \leqslant j \leqslant n$. We say that f *satisfies the Coleman criterion at p* if f is Hurwitz-integral at p, and $\mathrm{ord}_p(a_j) = 0$ for $j = k_i,\ 0 \leqslant i \leqslant s$, where k_i is as defined in (2). Furthermore, we say f *satisfies the Coleman criterion* if f satisfies the Coleman criterion at p for all p dividing n.

Remark 5. Note that if f satisfies the Coleman criterion at p, then $\mathrm{NP}(f,p) = \mathrm{NP}(e_n,p)$. Since f is Hurwitz-integral at p, the vertices of $\mathrm{NP}(f,p)$ lie on or above those of $\mathrm{NP}(e_n,p)$, and $\mathrm{ord}_p(a_j) = 0$ for $j = k_i,\ 0 \leqslant i \leqslant s$, implies that the vertices are in fact the same.

Proposition 6 (Coleman). *Suppose f satisfies the Coleman criterion at p and p^m divides n. Then p^m divides the degree of each factor of f over $\mathbb{Q}_p$.*

Proof. Write n as in (1). Since p^m divides n, $m \leqslant n_s$. From (3), p^m divides the denominator of each m_i. Then by Corollary 3, p^m divides the degree of each factor of f over $\mathbb{Q}_p$. □

Theorem 7. *If $f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{j!}$ in $\mathbb{Q}[x]$ satisfies the Coleman criterion, then f is irreducible over $\mathbb{Q}$.*

Proof. Write $n = \prod p^{n_p}$, the prime factorization of n. As noted in Remark 5, $\mathrm{NP}(f,p) = \mathrm{NP}(e_n,p)$ for all p such that $n_p > 0$. In particular, their slopes are the same. By Proposition 6, p^{n_p} divides the degree of each factor of f over $\mathbb{Q}_p$, and hence divides the degree of each factor over $\mathbb{Q}$. Since this is true for all p dividing n, n divides the degree of each factor of f over $\mathbb{Q}$. □

2. The Irreducibility of $L_n^{(-3-n)}(x)$

Since for our purposes we are concerned with $L_n^{(\alpha)}(x)$ when $\alpha = -r-1-n$ for various non-negative integers r, we introduce a more convenient parameterization.

Notation. For r a non-negative integer, let $\mathscr{L}_n^{(r)}(x) = L_n^{(-r-1-n)}(x)$. One can check that

$$\mathscr{L}_n^{(r)}(x) = \sum_{j=0}^{n} \frac{(n-j+1)(n-j+2)\cdots(n-j+r)}{r!}\frac{x^j}{j!}.$$

Proposition 8. *If p is a prime divisor of n and p does not divide $r!$, then $\mathscr{L}_n^{(r)}(x)$ satisfies the Coleman criterion at p.*

Proof. Clearly, $\mathscr{L}_n^{(r)}(x)$ is Hurwitz-integral at p, since p does not divide $r!$. Let $j = k_i$, as defined in (2). We have

$$\operatorname{ord}_p(a_{k_i}) = \operatorname{ord}_p(n-k_i+1) + \operatorname{ord}_p(n-k_i+2) + \cdots + \operatorname{ord}_p(n-k_i+r).$$

For $i = 0, 1, \ldots, s-1$, p divides $n - k_i = b_{i+1}p^{n_{i+1}} + \cdots + b_s p^{n_s}$. Since p does not divide $r!$, p is certainly not less than r, and thus p does not divide $n - k_i + l$ for $1 \leqslant l \leqslant r$. Since $a_{k_s} = 1$, we have $\operatorname{ord}_p(a_{k_i}) = 0$ for $0 \leqslant i \leqslant s$. □

Combining this with Theorem 7, we have

Corollary 9. *If $(n, r!) = 1$, then $\mathscr{L}_n^{(r)}(x)$ is irreducible over $\mathbb{Q}$.*

The main result of this section is a strengthening of the above for $r = 2$, namely

Theorem 10. *$\mathscr{L}_n^{(2)}(x)$ is irreducible for all $n \geqslant 1$.*

For n odd, $\mathscr{L}_n^{(2)}(x)$ is irreducible by Corollary 9. For $n \equiv 0 \bmod 4$, we claim that $\mathscr{L}_n^{(2)}(x)$ satisfies the Coleman criterion at $p = 2$, and thus is irreducible by Proposition 8 and Theorem 7. We have $a_j = \frac{(n-j+1)(n-j+2)}{2}$, and we wish to show that $\operatorname{ord}_2(a_j) = 0$ for $j = k_i$, as in (2).

By assumption, $n \equiv k_i \equiv 0 \bmod 4$, for $0 \leqslant i \leqslant s$. Hence, $(n-k_i+1)(n-k_i+2) \equiv (1)(2) \bmod 4$, which implies that $\frac{(n-k_i+1)(n-k_i+2)}{2} \equiv 1 \bmod 2$.

We are left with $n \equiv 2 \bmod 4$. This case requires some additional lemmas.

Notation. For the remainder of the proof, we write $n = 2k$, where k is odd.

Lemma 11. *If $\mathscr{L}_n^{(2)}(x)$ does not have a factor of degree k over $\mathbb{Q}$, then it is irreducible over $\mathbb{Q}$.*

Proof. Let $g(x)$ be any factor of $\mathscr{L}_n^{(2)}(x)$ over $\mathbb{Q}$. For any prime p that divides k, by Proposition 8, $\mathrm{NP}(\mathscr{L}_n^{(2)}, p) = \mathrm{NP}(e_n, p)$. As in the proof of Theorem 7, we can

conclude that k must divide the degree of g. Hence the only possible degrees for g are k and $2k$. $\square$

To eliminate the possibility of a degree $k=\frac{n}{2}$ factor, we apply the following Lemma due to Filaseta.

Lemma 12 (Filaseta). *Suppose $a_0, a_1, \ldots, a_n$ are integers with $|a_0|=1$. Let*

$$f(x)=\sum_{j=0}^{n} a_j \frac{x^j}{j!}.$$

Let m be a positive integer $\leqslant \frac{n}{2}$. If there exists a prime $p \geqslant m+1$ and a positive integer r such that

$$p^r \mid n(n-1)\cdots(n-m+1),$$

and p^r does not divide a_n, then f cannot have a factor of degree m over $\mathbb{Q}$.

The proof relies on a theorem of Dumas [3], to the effect that the Newton Polygon of the product of two polynomials is the Minkowski sum of their respective Newton Polygons. See [5] for details.

Lemma 13. *For $n \geqslant 14$, there exists a prime p such that $\frac{n+2}{2}<p<n-2$.*

Proof. Schur [15, p. 143] proved that for any real number $r \geqslant 29$, there exists a prime p such that $r<p\leqslant \frac{5}{4}r$. Let $r=\frac{4(n-3)}{5}$. Then for $n>39$, there exists p such that $\frac{n+2}{2}<\frac{4}{5}(n-3)<p\leqslant n-3<n-2$. The reader can easily check the lemma for $14\leqslant n\leqslant 39$. $\square$

Assume $n \geqslant 14$. We now show that $\mathscr{L}_n^{(2)}(x)$ has no factor of degree k. Let

$$A=\frac{(n+1)(n+2)}{2}.$$

Then we consider

$$f(x)=\frac{1}{A}\mathscr{L}_n^{(2)}(Ax)=\sum_{j=0}^{n} b_j \frac{x^j}{j!},$$

where $b_j = A^{j-1}\frac{(n-j+1)(n-j+2)}{2}$ for $1\leqslant j\leqslant n$, and $b_0=1$. Note that the b_j are all integers. By Lemma 13, there exists a prime p in the set

$$\left\{\frac{n+2}{2}+1, \frac{n+2}{2}+2, \ldots, n-3\right\} \subset \{n-k+1, n-k+2, \ldots, n\}.$$

We have

$$b_n = \left[\frac{(n+1)(n+2)}{2}\right]^{n-1}.$$

Since $2p$ is greater than $n+2$, p does not divide $n+1$ or $n+2$, hence does not divide b_n. Then by Lemma 12, $f(x)$ has no factor of degree k. It is clear that $f(x)$ has no factor of degree k if and only if $\mathscr{L}_n^{(2)}(x)$ has no factor of degree k.

We have now shown that $\mathscr{L}_n^{(2)}(x)$ is irreducible for all n except for 2, 6, and 10 (recall that $n \equiv 2 \bmod 4$). In these cases, $\mathscr{L}_n^{(2)}(x)$ is irreducible modulo the primes 5, 13, and 109, respectively. This completes the proof of Theorem 10.

3. Galois group calculations

We denote the Galois group of $\mathscr{L}_n^{(r)}(x)$ by $G_n(r)$. In this section, we describe Coleman's calculation of $G_n(0)$, and apply his techniques to prove

Theorem 14. *For $n \geqslant 1$,*

$$G_n(2) = \begin{cases} A_n & \text{if } n = 4k(k+1), \text{ for } k \text{ a positive integer.} \\ S_n & \text{otherwise.} \end{cases}$$

We will make use of the following three facts:

Theorem 15 (Jordan). *If G is a transitive subgroup of S_n which contains a p-cycle for some prime p strictly between $\frac{n}{2}$ and $n-2$, then $A_n \subseteq G$.*

See [9, Note C] and [10, Theorem 1] for a proof.

Theorem 16 (Chebyshev [1]). *For each integer $n \geqslant 8$, there exists a prime number p strictly between $\frac{n}{2}$ and $n-2$.*

Lemma 17. *The Galois group of a separable polynomial of degree n is contained in A_n if and only if its discriminant is a square.*

In addition, the following formula was computed by Schur [15, p. 229].

Theorem 18. *Let $\Delta(\alpha)$ denote the discriminant of $L_n^{(\alpha)}(x)$, for $\alpha \in \mathbb{Q}$. Then*

$$\Delta(\alpha) = n! \prod_{j=1}^{n} (jc_j)^{j-1}, \text{ where } c_j = \alpha + j.$$

3.1. The Galois group of the exponential Taylor polynomials

The following proposition can be obtained as a corollary to Coleman's calculation of the Newton polygon of $e_n(x)$ at an arbitrary prime p. Again, we write $n = b_1 p^{n_1} + b_2 p^{n_2} + \cdots + b_s p^{n_s}$, as in (1).

Proposition 19 (Coleman). *Suppose $p^k \leqslant n$. Then p^k divides the degree of the splitting field of $e_n(x)$ over $\mathbb{Q}_p$.*

Proof. If $p^k \leqslant n$, we must have $k \leqslant n_1$. So p^k divides the denominator of the first slope $m_1 = \frac{-(p^{n_1}-1)}{p^{n_1}(p-1)}$, as calculated in (3). Let α be a root of $e_n(x)$ such that $\mathrm{ord}_p(\alpha) = -m_1$. By the proof of Corollary 3, p^k divides the degree of the extension $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$, and hence p^k divides the degree of the splitting field of $e_n(x)$ over $\mathbb{Q}_p$. □

Corollary 20. *Suppose $\frac{n}{2} < p \leqslant n$ is a prime number. Then $G_n(0)$ contains a p-cycle.*

Proof. By the previous proposition, p divides the degree of the splitting field of $e_n(x)$ over $\mathbb{Q}_p$, which in turn divides the degree of the splitting field of $e_n(x)$ over $\mathbb{Q}$. Thus p divides the order of $G_n(0)$. Cauchy's theorem implies that $G_n(0)$ contains an element of order p. Since $p > \frac{n}{2}$, the only elements of order p in S_n are p-cycles. □

Combining the facts above, we have that for $n \geqslant 8$, $G_n(0) = A_n$ if the discriminant of $e_n(x)$ is a square, and $G_n(0) = S_n$ otherwise. This allowed Coleman to prove the following theorem, which Schur [15, No. 67] had previously obtained using other techniques.

Theorem 21 (Schur, Coleman). *For $n \geqslant 8$,*

$$G_n(0) = \begin{cases} A_n & \text{if } n \equiv 0 \bmod 4, \\ S_n & \text{otherwise.} \end{cases}$$

The following was obtained by Schur's method, and will be useful to us later.

Theorem 22 (Hajir [8]). *For $n \geqslant 14$,*

$$G_n(1) = \begin{cases} A_n & \text{if } n \equiv 1 \bmod 4, \\ S_n & \text{otherwise.} \end{cases}$$

3.2. Proof of Theorem 14

Essentially the same argument as above applies in our case. First, suppose $n \geqslant 14$ and p is a prime satisfying $\frac{n+2}{2} < p < n-2$, which exists by Lemma 13.

Proposition 23. *The Galois group of $\mathscr{L}_n^{(2)}(x)$ contains a p-cycle.*

Proof. It suffices to show that $\mathscr{L}_n^{(2)}(x)$ satisfies the Coleman criterion at p. Indeed, we would then know that the Newton polygon at p of $\mathscr{L}_n^{(2)}(x)$ is the same as that of $e_n(x)$ (see Remark 5). The proofs of Proposition 19 and Corollary 20 clearly apply to any polynomial whose Newton polygon at p coincides with that of $e_n(x)$, giving us that $G_n(2)$ contains a p-cycle.

To show that $\mathscr{L}_n^{(2)}(x)$ satisfies the Coleman criterion at p, we note that the p-adic expansion of n is $p^1+(n-p)p^0$, since $n<2p<p^2$. In this case, we have $k_0=0$, $k_1=p$, and $k_2=n$. We must show that $\mathrm{ord}_p(a_{k_i})=0$ for $i=0,1$, and 2, where $a_j=\frac{(n-j+1)(n-j+2)}{2}$. Since $2p>n+2$, it is clear that $\mathrm{ord}_p(a_0)=0$. Now consider $a_p=\frac{(n-p+1)(n-p+2)}{2}$. Since $n-p+1$ and $n-p+2$ are both less than n, $\mathrm{ord}_p(a_p)>0$ implies that $p=n-p+1$ or $p=n-p+2$, i.e., $p=\frac{n+1}{2}$ or $p=\frac{n+2}{2}$, which is not possible. Finally, $a_n=1$, and the proof is complete. □

Hence, for $n\geqslant 14$, we have that $G_n(2)$ is A_n if the discriminant is a square, and S_n otherwise.

Notation. For a,b in $\mathbb{Q}$, we write $a\sim b$ if $a=bc^2$ for some c in $\mathbb{Q}$.

Using Theorem 18, we calculate:

$$\begin{aligned}\Delta(-3-n)&=n!\prod_{j=1}^{n}j^{j-1}(-3-n+j)^{j-1}\\&=n!\cdot 2\cdot 3^2\cdots n^{n-1}\cdot(-1-n)(-n)^2\cdots(-4)^{n-2}(-3)^{n-1}\\&=2^2\cdot 3^3\cdots n^n\cdot(-1)^{\frac{n(n-1)}{2}}(n+1)(n)^2(n-1)^3\cdots 4^{n-2}\cdot 3^{n-1}.\end{aligned}$$

If n is odd,

$$\Delta(-3-n)\sim(-1)^{\frac{n(n-1)}{2}}\frac{(n+1)!}{2}.$$

Regardless of sign, $\Delta(-3-n)$ cannot be a square for n odd, since for $n\geqslant 14$ there is a prime p such that p divides $(n+1)!$, but p^2 does not.

If n is even,

$$\begin{aligned}\Delta(-3-n)&\sim(-1)^{\frac{n(n-1)}{2}}(n+1)\\&\sim\begin{cases}(n+1) & \text{if } n\equiv 0 \bmod 4,\\ -(n+1) & \text{if } n\equiv 2 \bmod 4.\end{cases}\end{aligned}$$

Obviously, $\Delta(-3-n)$ is not a square for $n \equiv 2 \bmod 4$. For $n \equiv 0 \bmod 4$, it is easy to check that $n+1$ is a square if and only if $n = 4k(k+1)$ for some positive integer k.

To complete the proof of Theorem 14, we must only check the cases $1 \leqslant n \leqslant 13$. The argument above holds for $n = 10$ and 11, since for these values of n there is a prime p in the desired range. For $n \leqslant 9$, the statement can be verified using the PARI routine `polgalois`. Finally, for $n = 12$ and $n = 13$, it suffices to check that in both cases, $NP_7(\mathscr{L}_n^{(2)}(x))$ has one slope whose denominator is divisible by 7. From the proof of Corollary 3, we deduce that $p = 7$ divides the order of $G_n(2)$, and hence A_n is contained in $G_n(2)$ by Theorem 15.

4. The embedding problem

In this section, we describe Feit's application of a theorem of Serre to certain generalized Laguerre polynomials, which allowed him to construct explicitly fields with Galois group isomorphic to the double cover of A_n for certain values of n. Refer to [4] for details.

4.1. Feit's Formula

To describe the setup, we follow Section 2 of [4] closely. Let $f(x) \in \mathbb{Q}[x]$ be a monic, irreducible polynomial of degree n. Then we have a field $E \coloneqq \mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\theta)$, where θ is a root of f. On the other hand, if E is a finite separable extension of $\mathbb{Q}$, then $E = \mathbb{Q}(\theta)$ for some θ in E. Thus $E \simeq \mathbb{Q}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of θ over $\mathbb{Q}$, so E can be viewed as an n-dimensional vector space over $\mathbb{Q}$.

Given any α in such a field E, let $\mathrm{Tr}_{E/\mathbb{Q}}(\alpha)$ be the trace of the "multiplication by α" map. The function $\alpha \mapsto \mathrm{Tr}_{E/\mathbb{Q}}(\alpha^2)$ is a non-degenerate quadratic form on E with values in $\mathbb{Q}$, which we will denote $Q(f)$. This is the quadratic form that appears in Serre's Theorem.

Definition 24. Write $f(x) = \prod_{j=1}^{n}(x-\theta_j)$, where $\theta_1 = \theta$. For all t such that $1 \leqslant t \leqslant n$, define the $t \times n$ matrix

$$A_t = A_t(f) = (a_{ij}) = (\theta_j^{i-1}), \quad 1 \leqslant i \leqslant t, \quad 1 \leqslant j \leqslant n.$$

The matrix A_n is known as the *Vandermonde matrix* for f, and

$$\det(A_n) = \prod_{i<j} (\theta_i - \theta_j).$$

Furthermore, define

$$D_t = D_t(f) = A_t A_t^T$$

and

$$\Delta_t = \Delta_t(f) = \det(D_t).$$

One checks immediately that

Proposition 25. *The matrix for $Q(f)$ with respect to the basis $\{1, \theta, \ldots, \theta^{n-1}\}$ is precisely D_n.*

Furthermore, we have the following:

Theorem 26. *Suppose $\Delta_t \neq 0$ for $1 \leqslant t \leqslant n$. Then $Q(f)$ is equivalent over $\mathbb{Q}$ to $a_1x_1^2 + \cdots + a_nx_n^2$, where $a_1 = \Delta_1 = n$, and $a_t = \frac{\Delta_t}{\Delta_{t-1}}$, for $2 \leqslant t \leqslant n$.*

Let (K^n, Q) be a non-degenerate quadratic module over the field K, where K is either $\mathbb{Q}_p$ for a prime p, or $\mathbb{R}$, which corresponds to $p = \infty$. If Q is equivalent to $b_1x_1^2 + b_2x_2^2 + \cdots + b_nx_n^2$ over K, then the *Hasse–Witt Invariant* of Q is defined by

$$\varepsilon_p(Q) = \prod_{i<j} (b_i, b_j)_p = \pm 1,$$

where $(\cdot, \cdot)_p$ denotes the Hilbert symbol at p. It can be shown that the Hasse-Witt invariant does not depend on choice of orthogonal basis. For details, see [16]. For p a prime or $p = \infty$, let $\varepsilon_p(f)$ denote the Hasse–Witt invariant of $Q(f)$ considered as a quadratic form over $\mathbb{Q}_p$.

Theorem 27. *Define $\Delta_0 = 1$ and suppose that $\Delta_t \neq 0$ for $1 \leqslant t \leqslant n$. Then*

$$\varepsilon_p(f) = \left(-1, \prod_{j=1}^{n-1} \Delta_j\right)_p \left\{\prod_{j=1}^{n} (\Delta_{j-1}, \Delta_j)_p\right\}$$

for all primes p and $p = \infty$.

Feit studied generalized Laguerre polynomials in particular, and was able to derive an explicit formula that enables us to calculate their Hasse–Witt invariants. The result is

Theorem 28 (Feit). *Let $\Delta_t(\alpha)$ be $\Delta_t(f)$ for $f(x) = L_n^{(\alpha)}(x)$, as defined above. Then for $1 \leqslant t \leqslant n$,*

$$\Delta_t(\alpha) = \prod_{j=n-t+1}^{n} j(jc_j)^{j-(n-t+1)}, \text{ where } c_j = \alpha + j.$$

4.2. Serre's Theorem

For $n \geqslant 5$, $\tilde{A}_n$ will denote the double cover of A_n, i.e., the group for which there exists a non-split exact sequence

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \tilde{A}_n \to A_n \to 1.$$

The group $\tilde{A}_n$ is unique up to isomorphism. See [11] for details. On the other hand, S_n has two non-isomorphic double covers, which we denote by $\tilde{S}_n{}^+$ and $\tilde{S}_n{}^-$. In both cases, we have a non-split exact sequence

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \tilde{S}_n{}^{\pm} \to S_n \to 1.$$

The distinction between the two groups has to do with transpositions in S_n. Transpositions lift to elements of order 2 in $\tilde{S}_n{}^+$, i.e., the preimages of transpositions in $\tilde{S}_n{}^+$ have order 2. In $\tilde{S}_n{}^-$, transpositions lift to elements of order 4. More details can be found in [13].

Theorem 29 (Serre [17]). *Let L be the splitting field of $f \in \mathbb{Q}[x]$, and let G be the Galois group of L over $\mathbb{Q}$. Fix $G \subseteq S_n$, where n is the degree of f, and let $\tilde{G}^{\pm}$ be the inverse image of G in $\tilde{S}_n{}^{\pm}$. Then the following are equivalent*:

(i) *There exists a quadratic extension field M of L which is a Galois extension of $\mathbb{Q}$ with* $\mathrm{Gal}(M/\mathbb{Q}) \simeq \tilde{G}^{\pm}$.
(ii) $\varepsilon_p(f)(\pm 2, \Delta_n)_p = 1$ *for all primes p and $p = \infty$.*

An alternate proof can be found in Ledet [13]. For simplicity of notation, we define

$$\mathscr{S}_p^+(f) = \varepsilon_p(f)(2, \Delta_n)_p,$$

and

$$\mathscr{S}_p^-(f) = \varepsilon_p(f)(-2, \Delta_n)_p.$$

Remark 30. If $G \subseteq A_n$, then $\tilde{G}^+$ is isomorphic to $\tilde{G}^-$, and we need only consider $\tilde{G}$, the inverse image of G in $\tilde{A}_n$. Note that in this case, $\Delta_n(f)$ is a square, so $\mathscr{S}_p^+(f) = \mathscr{S}_p^-(f) = \varepsilon_p(f)$.

Feit applied Serre's Theorem to $L_n^{(\alpha)}(x)$ for $\alpha = 1$ via Theorem 28, and Hajir [8] did the same for $\mathscr{L}_n^{(r)}(x)$ with $r = 0$ and 1. Continuing along this line, we will prove the following:

Theorem 31. *The splitting field of $\mathscr{L}_n^{(2)}(x)$ can be embedded in a field M with Galois group isomorphic to $\tilde{A}_n$ if and only if $n = 4k(k+1)$, for k a positive integer.*

In light of Serre's Theorem and Theorem 14, this follows from the proposition below, coupled with the following observation: If $n = 4k(k+1)$ for a positive integer k, then $n+1$ is an odd square, and n is congruent to 0 modulo 8.

In proving this proposition, we will often make use of the standard properties of the Hilbert symbol, as listed in [4, p. 235]. Some elementary steps will be left to the reader.

Proposition 32. *Suppose* $n \equiv 0 \bmod 4$. *If for all primes* $q \equiv 3 \bmod 4$ *such that* q *divides* $n+1, ord_q(n+1) \equiv 0 \bmod 2$, *then*

$$\mathscr{S}_p^+(\mathscr{L}_n^{(2)}(x)) = \begin{cases} 1 & \text{if } n \equiv 0 \bmod 8, \\ (-1,-1)_p & \text{if } n \equiv 4 \bmod 8. \end{cases}$$

Proof. Set $\Delta_t := \Delta_t(-3-n)$. By Theorem 28,

$$\Delta_t = n^t(n-1)^{t-1}\cdots(n+1-t)\cdot(-3)^{t-1}(-4)^{t-2}\cdots(-(t+1)). \tag{4}$$

Write

$$\begin{aligned}\prod_{t=1}^{n-1}\Delta_t &= \left\{\prod_{\text{odd } t}\Delta_t\right\}\left\{\prod_{\text{even } t}\Delta_t\right\} \\ &\sim \{(-1)^{\frac{n}{4}}n(n-2)\cdots 4\cdot 2\}\{(-1)^{\frac{n}{4}}\} \\ &\sim n(n-2)\cdots 4\cdot 2.\end{aligned}$$

Due to the multiplicative properties of the Hilbert Symbol, we may write

$$\prod_{t=1}^{n}(\Delta_{t-1},\Delta_t)_p = \prod_{k=1}^{\frac{n}{2}}(\Delta_{2k-1},\Delta_{2k-2}\Delta_{2k})_p.$$

Define $z_0 = (-1,\prod_{t=1}^{n-1}\Delta_t)_p$, and $z_k = (\Delta_{2k-1},\Delta_{2k-2}\Delta_{2k})_p$, for $1 \leqslant k \leqslant \frac{n}{2}$. So, by Theorem 27,

$$\mathscr{S}_p^+(\mathscr{L}_n^{(2)}(x)) = (2,\Delta_n)_p\prod_{k=0}^{\frac{n}{2}}z_k.$$

We calculate:

$$\Delta_{2k-1} \sim (-1)^{k-1}n(n-2)\cdots(n+2-2k)\cdot 4\cdot 6\cdots 2k,$$

$$\Delta_{2k} \sim (-1)^k(n-1)(n-3)\cdots(n+1-2k)\cdot 3\cdot 5\cdots(2k+1),$$

$$\Delta_{2k-2} \sim (-1)^{k-1}(n-1)(n-3)\cdots(n+3-2k)\cdot 3\cdot 5\cdots(2k-1),$$

so that for $1 \leqslant k \leqslant \frac{n}{2}$,

$$z_k = ((-1)^{k-1} n(n-2)\cdots(n+2-2k)\cdot 4\cdot 6\cdots 2k, -(2k+1)(n+1-2k))_p. \quad (5)$$

The involution $k \leftrightarrow \frac{n-2k}{2}$ has the unique fixed point $\frac{n}{4}$ on the set $\{1,\ldots,\frac{n-2}{2}\}$. Write

$$\mathscr{S}_p^+(\mathscr{L}_n^{(2)}(x)) = z_0 z_{\frac{n}{4}} z_{\frac{n}{2}} (2, \Delta_n)_p \prod_{k=1}^{\frac{n-4}{4}} z_k z_{\frac{n-2k}{2}}.$$

One can check that $z_k z_{\frac{n-2k}{2}} = 1$ for $1 \leqslant k \leqslant \frac{n-4}{4}$. Using (4), (5), and the fact that $(-1,2)_p = 1$ for all primes p and $p = \infty$,we calculate:

$$\begin{aligned} z_0 \cdot z_{\frac{n}{4}} &= (-1, n(n-2)\cdots 4\cdot 2)_p \cdot (-1, (-1)^{\frac{n-4}{4}} n(n-2)\cdots 6\cdot 4)_p \\ &= (-1, -1^{\frac{n-4}{4}})_p, \end{aligned}$$

$$\begin{aligned} z_{\frac{n}{2}} \cdot (2, \Delta_n)_p &= (-2, -(n+1))_p \cdot (2, n+1)_p \\ &= (-1, -(n+1))_p \cdot (2, -(n+1))_p \cdot (2, n+1)_p \\ &= (-1, -(n+1))_p. \end{aligned}$$

Thus,

$$\mathscr{S}_p^+(\mathscr{L}_n^{(2)}(x)) = \begin{cases} (-1, n+1)_p & \text{if } n \equiv 0 \bmod 8, \\ (-1, -(n+1))_p & \text{if } n \equiv 4 \bmod 8. \end{cases}$$

Now we need the following lemma, the proof of which is left to the reader.

Lemma 33. *For m a positive integer, $(-1,m)_p = 1$ for all p if and only if for every prime $q \equiv 3 \bmod 4$, $ord_q(m) \equiv 0 \bmod 2$.*

Observing that $(-1, -(n+1))_p = (-1,-1)_p \cdot (-1, n+1)_p$, the argument is complete. □

4.3. Summary of known results

The following tables provide a summary of calculations of the Hasse–Witt invariants for $\mathscr{L}_n^{(r)}(x)$ known to the author. The entries in bold indicate results concerning $\tilde{A}_n$, as opposed to $\tilde{S}_n^{\pm}$ (see Section 3). Unless otherwise indicated, calculations can be found in [19]. Note that the entries in Table 2 are easily obtained

Table 1
Values of $\mathscr{S}_p^+(\mathscr{L}_n^{(r)}(x))$ for some congruence classes of n modulo 8

$n \bmod 8$	$r=0$	$r=1$	$r=2$
0	**1**[a]		**1**[b],$(-1,n+1)_p$[c]
1		**1**[a]	
2	1		1
3		1	
4	$(-1,-1)_p$[a]		$(-1,-n-1)_p$
5		$(-1,-1)_p$[a]	
6	$(-1,-1)_p$		$(-1,-1)_p$
7		$(-1,-1)_p$	

[a] Due to Hajir [8].
[b] Corresponds to $\tilde{A}_n$ if $n=4k(k+1)$.
[c] Is trivial if for all primes $q \equiv 3 \bmod 4$ such that $q|n+1$, $\mathrm{ord}_q(n+1) \equiv 0 \bmod 2$.

Table 2
Values of $\mathscr{S}_p^-(\mathscr{L}_n^{(r)}(x))$ for some congruence classes of n modulo 8

$n \bmod 8$	$r=0$	$r=1$	$r=2$
0	**1**		**1**[a]
1		**1**	
2	$(-1,-1)_p$		$(-1,-n-1)_p$
3		$(-1,-1)_p$	
4	$(-1,-1)_p$		$(-1,-1)_p$
5		$(-1,-1)_p$	
6	1		$(-1,n+1)_p$[b]
7		1	

[a] Corresponds to $\tilde{A}_n$ if $n=4k(k+1)$.
[b] Is trivial if for all primes $q \equiv 3 \bmod 4$ such that $q|n+1$, $\mathrm{ord}_q(n+1) \equiv 0 \bmod 2$.

from those in Table 1, since

$$\mathscr{S}_p^-(f) = \mathscr{S}_p^+(f)(-1,\Delta_n)_p.$$

References

[1] P.I. Chebyshev, Sur la totalité des nombres premiers inférieurs à une limite donnée, J. Math. 17 (1852) 341–365.
[2] R.F. Coleman, On the Galois groups of the exponential Taylor polynomials, L'Enseignement Math. 33 (1987) 183–189.
[3] G. Dumas, Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels, J. Math. Pures Appl. 2 (1906) 191–258.
[4] W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields, J. Algebra 104 (1986) 231–260.

[5] M. Filaseta, A generalization of an irreducibility theorem of I. Schur, in: B.C. Berndt, H.G. Diamond, A.J. Hildebrand (Eds.), Analytic Number Theory, Vol. 1, Progr. Math. 138.
[6] M. Filaseta, T.-Y. Lam, On the irreducibility of the generalized Laguerre polynomials, Acta Arith. 105 (2) (2002) 177–182.
[7] R. Gow, Some generalized Laguerre polynomials whose Galois groups are the alternating groups, J. Number Theory 31 (1989) 201–207.
[8] F. Hajir, Some $\tilde{A}_n$-extensions obtained from generalized Laguerre polynomials, J. Number Theory 50 (1995) 206–212.
[9] C. Jordan, Traité des Substitutions et des Équations Algébriques, Gauthier-Villars, Paris, 1870.
[10] C. Jordan, Sur la limite de transitivité des groupes non alternés, Bull. Soc. Math. France 1 (1872–1873) 40–71.
[11] G. Karpilovsky, Projective representations of finite groups, Marcel Dekker, New York, 1985.
[12] N. Koblitz, *P*-adic numbers, *p*-adic analysis, and Zeta-functions, Springer, Berlin, 1984.
[13] A. Ledet, On a theorem by Serre, Proc. AMS 128 (1999) 27–29.
[14] G. Pólya, G. Szegő, Problems and Theorems in Analysis II, Springer, Berlin, 1976.
[15] I. Schur, Gemsammelte Abhandlungen, Vol. 3, Springer, Berlin, 1973.
[16] J.-P. Serre, A Course in Arithmetic, Springer, Berlin, 1973.
[17] J.-P. Serre, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, Comment. Math. Helv. 59 (1984) 651–676.
[18] E. Weiss, Algebraic Number Theory, Chelsea, London, 1963.
[19] E.A. Wrobel, On a Certain Class of Generalized Laguerre Polynomials, Master's Thesis, University of North Carolina at Chapel Hill, 2003.